Alternative Approaches: Quantum Cryptography

A. Würfl

17th April 2005

Heisenberg´s Uncertainty Principle

Werner Heisenberg (1927):

Measuring two conjugate variables it is impossible to determine both values with higher accuracy than a given lower boundary.

This means:
measuring a quantum system in general disturbs it and yields incomplete information about its state before the measurement.

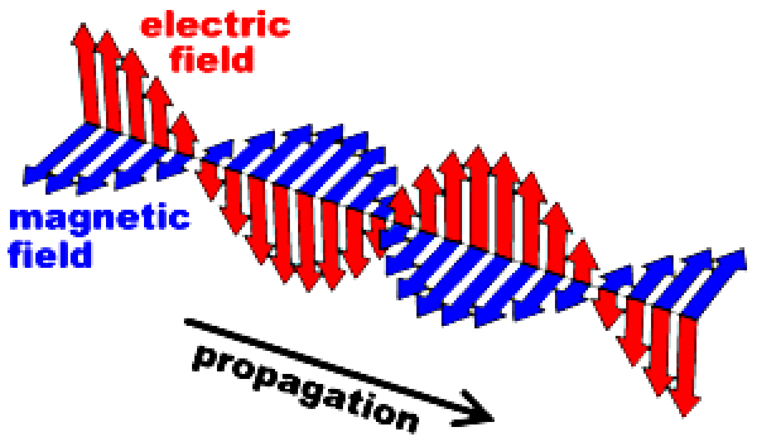
Example

The simultaneous measurement of a particle's position and momentum.

The Polarization of Light

The Nature of Light

- Light consists of transverse electromagnetic waves.
- The electric and the magnetic fields are perpendicular to the direction in which they propagate.
- The electric and magnetic fields are perpendicular to each other, too.


electric
field
magnetic
field
propagation

Missionstatement

Objective

We want to encode a bit in the direction of polarization of a photon.

Solution:

Create a photon in a particular polarization state using a polarizer.

The 2^{nd} important Law of Nature

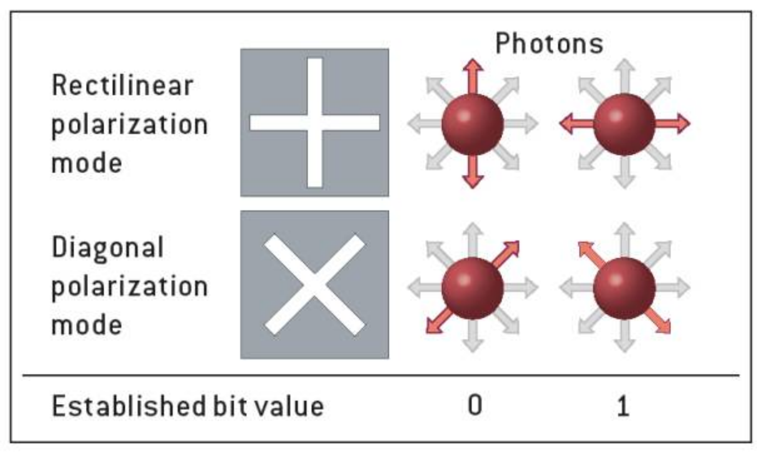
Polarization

If the axis of the polarizer makes an angle of θ with the plane of the electric field of the photon fed into the polarizer, there is a probability of $\cos^2\theta$ that the photon will emerge with its polarization set at the desired angle and a probability of $1 - \cos^2\theta$ that it will be absorbed.

Alice Eve

Definition

Using polarizers in certain alignments we can obtain photons oscillating in a plane at either 0° or 90° to some reference line (”rectilinear”) or oscillating in a plane at 45° or 135° (”diagonal”). Photons oscillating at angels of 0° or 45° represent the binary value 0 and those polarized at angles of 90° or 135° represent the binary value 1.


Photons
Rectilinear polarization mode
Diagonal polarization mode
Established bit value
0
1

Quantum Cryptography in the Absence of Eavesdropping

Objective

Alice and Bob want to exchange a **secret key**.

Using the follwing protocol they can limit the probability of undetected eavesdropping to any given upper bound.

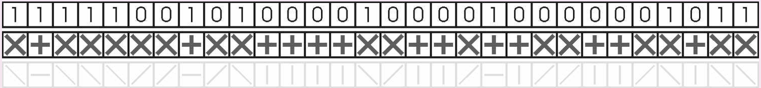
Step 1: Generating a random bit-sequence and random polarizer orientations

Alice generates a random bit-sequence:

1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1
×	+	×	×	×	×	×	+	×	×	+	+	+	+	×	×	+	+	×	+	+	×	×	+	+	×	×	+	×	×
\	—	\	\	\	/	/	—	/	\	ǀ	ǀ	ǀ	ǀ	\	/	ǀ	ǀ	/	—	ǀ	/	/	ǀ	ǀ	/	\	ǀ	\	\

Step 1: Generating a random bit-sequence and random polarizer orientations

Alice generates a random sequence of polarizer orientations:



Step 1: Generating a random bit-sequence and random polarizer orientations

Alice encodes her bits . . .

1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1
×	+	×	×	×	×	×	+	×	×	+	+	+	+	×	×	+	+	×	+	+	×	×	+	+	×	×	+	×	×
╲	─	╲	╲	╲	╱	╱	─	╱	╲	│	│	│	│	╲	╱	│	│	╱	─	│	╱	╱	│	│	╱	╲	│	╲	╲

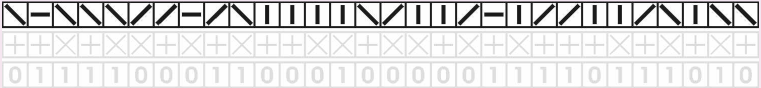
Step 1: Generating a random bit-sequence and random polarizer orientations

. . . and sends them to Bob:

1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1
×	+	×	×	×	×	×	+	×	×	+	+	+	+	×	×	+	+	×	+	+	×	×	+	+	×	×	+	×	×
\	−	\	\	\	/	/	−	/	\	|	|	|	|	\	/	|	|	/	−	|	/	/	|	|	/	\	|	\	\

Step 2: Measuring the photons using random polarizer orientations

Bob receives the polarized photons:



What happend?

Step 2: Measuring the photons using random polarizer orientations

Bob generates a random sequence of polarizer orientations to measure the polarization:

╲	—	╲	╲	╲	╱	╱	—	╱	╲	│	│	│	│	╲	╱	│	│	╱	—	│	╱	╱	│	│	╱	╲	│	╲	╲
+	+	×	+	×	×	+	×	+	×	+	+	×	×	+	×	×	+	×	+	×	+	+	+	×	+	×	+	×	+
0	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	1	1	1	0	1	0

What happend?

Step 2: Measuring the photons using random polarizer orientations

Bob decodes the measured orientations into bits:

<table>
<tr><td>\</td><td>—</td><td>\</td><td>\</td><td>\</td><td>/</td><td>/</td><td>—</td><td>/</td><td>\</td><td>|</td><td>|</td><td>|</td><td>|</td><td>\</td><td>/</td><td>|</td><td>|</td><td>/</td><td>—</td><td>|</td><td>/</td><td>/</td><td>|</td><td>|</td><td>/</td><td>\</td><td>|</td><td>\</td><td>\</td></tr>
<tr><td>+</td><td>+</td><td>×</td><td>+</td><td>×</td><td>×</td><td>+</td><td>×</td><td>+</td><td>×</td><td>+</td><td>+</td><td>×</td><td>×</td><td>+</td><td>×</td><td>×</td><td>+</td><td>×</td><td>+</td><td>×</td><td>+</td><td>+</td><td>+</td><td>×</td><td>+</td><td>×</td><td>+</td><td>×</td><td>+</td></tr>
<tr><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td></tr>
</table>

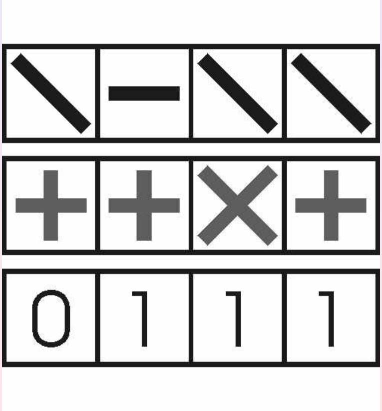
What happend?

Step 2: Measuring the photons using random polarizer orientations

What happend?

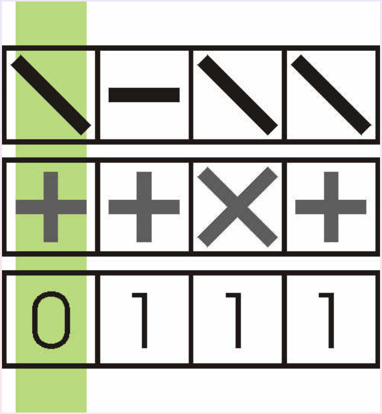
A closer Look

1. Bob chose the wrong polarizer ⇒ Bob measueres random value for the first bit ▸ Why?
2. Bob chose the right polarizer ⇒ Bob measures the correct value for the second bit
3. Bob measures correct value
4. Bob measures random value
5. ...



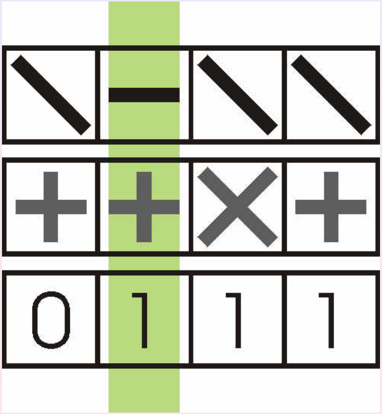
A closer Look

1. Bob chose the wrong polarizer $\Rightarrow$ Bob measueres random value for the first bit ▸ Why?
2. Bob chose the right polarizer $\Rightarrow$ Bob measures the correct value for the second bit
3. Bob measures correct value
4. Bob measures random value
5. . . .



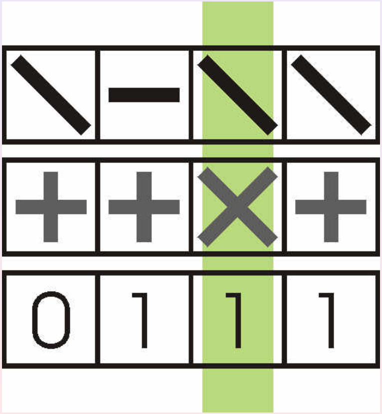
A closer Look

1. Bob chose the wrong polarizer $\Rightarrow$ Bob measueres random value for the first bit ▸ Why?
2. Bob chose the right polarizer $\Rightarrow$ Bob measures the correct value for the second bit
3. Bob measures correct value
4. Bob measures random value
5. ...



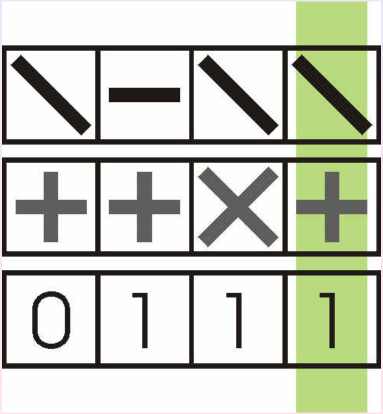
A closer Look

1. Bob chose the wrong polarizer $\Rightarrow$ Bob measueres random value for the first bit ▸ Why?
2. Bob chose the right polarizer $\Rightarrow$ Bob measures the correct value for the second bit
3. Bob measures correct value
4. Bob measures random value
5. ...



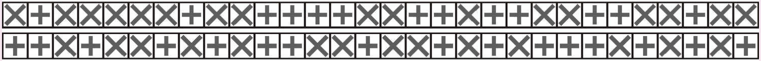
A closer Look

1. Bob chose the wrong polarizer
   ⇒ Bob measueres random value for the first bit Why?
2. Bob chose the right polarizer
   ⇒ Bob measures the correct value for the second bit
3. Bob measures correct value
4. Bob measures random value
5. ...



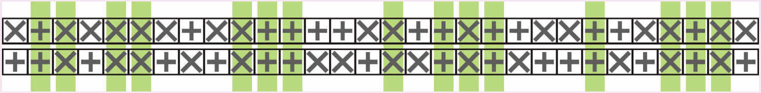
Step 3: Comparing the used polarizer orientations

Using a public insecure channel Alice and Bob compare their used polarizer orientations and agree on a random subset of the matching polarizer orientations:



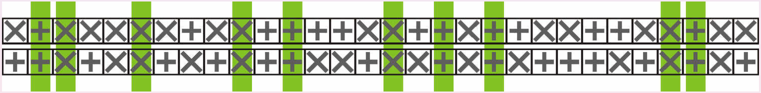
Step 3: Comparing the used polarizer orientations

Using a public insecure channel Alice and Bob compare their used polarizer orientations and agree on a random subset of the matching polarizer orientations:



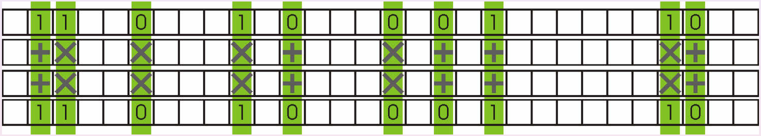
Step 3: Comparing the used polarizer orientations

Using a public insecure channel Alice and Bob compare their used polarizer orientations and agree on a random subset of the matching polarizer orientations:



Step 4: Comparing a subset of bits

For those bits Alice uses the public channel to tell Bob what he should have measured.



Eavesdropping

If there was no eavesdropping Bob has measured the same values.

Step 5: Retrieving the common secret key

If Alice and Bob agree on the exchanged bits the connection can be considered secure.

Alice and Bob now have a common bit-sequence. Part of this sequence was used to detect possible eavesdropping.
They use the rest of the sequence as their common secret key:

Step 5: Retrieving the common secret key

If Alice and Bob agree on the exchanged bits the connection can be considered secure.

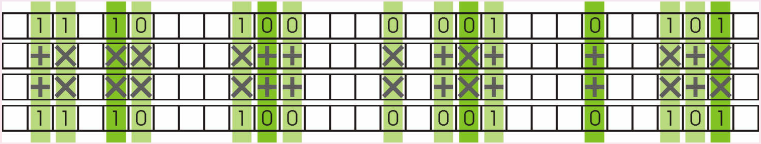
Alice and Bob now have a common bit-sequence. Part of this sequence was used to detect possible eavesdropping.
They use the rest of the sequence as their common secret key:

	1	1		1	0				1	0	0				0		0	0	1				0			1	0	1	
	+	×		×	×				×	+	+				×		+	×	+				+			×	+	×	
	+	×		×	×				×	+	+				×		+	×	+				+			×	+	×	
	1	1		1	0				1	0	0				0		0	0	1				0			1	0	1	

Step 5: Retrieving the common secret key

If Alice and Bob agree on the exchanged bits the connection can be considered secure.

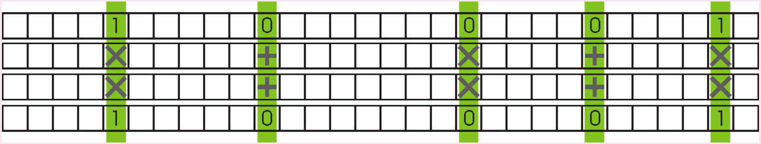
Alice and Bob now have a common bit-sequence. Part of this sequence was used to detect possible eavesdropping.
They use the rest of the sequence as their common secret key:



Step 5: Retrieving the common secret key

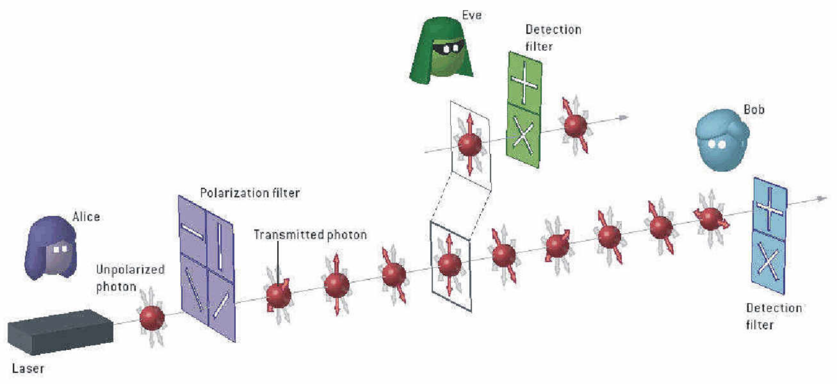
If Alice and Bob agree on the exchanged bits the connection can be considered secure.

Alice and Bob now have a common bit-sequence. Part of this sequence was used to detect possible eavesdropping.
They use the rest of the sequence as their common secret key:



Quantum Cryptography in the Presence of Eavesdropping

Quantum Cryptography in the Presence of Eavesdropping



Eve's Strategy

What can Eve do?

1. Eve intercepts the photons.
2. Eve uses random polarizer orientations to measure the photons.
3. Eve decodes the message according to her observations.
4. Eve passes the message on to Bob.

Where is the problem?

Eve's Effect on the Communication

According to **Heisenberg** Eve disturbs the quantum system by measuring it and hence looses information about its state before the measurement.

Example

Tow possible cases:

1. Eve uses the correct polarizer orientation $\Rightarrow$ No Problem!
2. Eve uses the wrong polarizer orientation
   $\Rightarrow$ Eve disturbs the system!

An Example

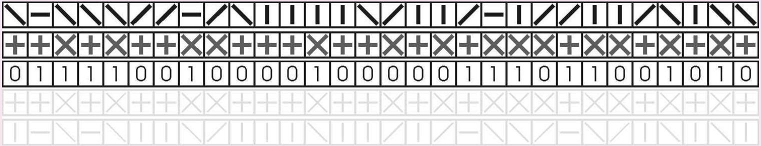
- Let's suppose Alice encoded 0 using the rectilinear polarizer.
- Eve uses the diagonal polarizer to measure this photon.
- Eve measures a random value. Why?
- Eve encodes the measured bit with the diagonal polarizer. As Bob uses the rectilinear polarizer he will also measure a random value.

Probabilities

1. Eve used the correct polarizer with probability $\frac{1}{2}$. In this case she will send on a photon with the same polarization plane and there is no possibility to detect her.
2. Eve used the wrong polarizer with probability $\frac{1}{2}$.
   She encodes the measured bit with this wrong polarizer orientation.
   - Bob measures a random value.
   - With probability of $\frac{1}{2}$ he will decode a bit different from the bit Alice sent. In this case he will know the presence of Eve.

Eve's Point of View

Eve intercepts the photons and uses random polarizer orientations for decoding



Eve's Point of View

Eve encodes the measured bits with her polarizer orientations and sends them on to Bob

╲	─	╲	╲	╲	╱	╱	─	╱	╲	│	│	│	│	╲	╱	│	│	╱	─	│	╱	╱	│	│	╱	╲	│	╲	╲
+	+	×	+	×	+	+	×	×	+	+	+	×	+	+	×	+	×	+	×	×	×	+	×	×	+	×	+	×	+
0	1	1	1	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1	1	0	0	1	0	1	0
+	+	×	+	×	+	+	×	×	+	+	+	×	+	+	×	+	×	+	×	×	×	+	×	×	+	×	+	×	+
│	─	╲	─	╲	│	│	╲	╱	│	│	│	╲	│	│	╱	│	╱	─	╲	╲	╱	─	╲	╱	│	╲	│	╲	│

The intercepted Message

Bob decodes the photons. . .

$\vert$	—	\	—	\	$\vert$	$\vert$	\	/	$\vert$	$\vert$	$\vert$	\	$\vert$	$\vert$	/	$\vert$	/	—	\	\	/	—	\	/	$\vert$	\	$\vert$	\	$\vert$
+	+	×	+	×	×	+	×	+	×	+	+	×	×	+	×	×	+	×	+	×	+	+	+	×	+	×	+	×	+
0	1	1	1	1	1	0	1	1	1	0	0	1	0	0	0	0	0	1	1	1	1	1	0	0	0	1	0	1	0

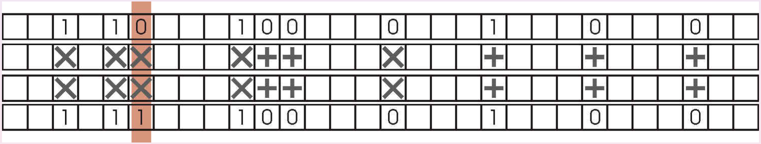
The intercepted Message

…compares with Alice…

		1		1	0				1	0	0				0				1				0				0		
		×		×	×				×	+	+				×				+				+				+		
		×		×	×				×	+	+				×				+				+				+		
		1		1	1				1	0	0				0				1				0				0		

The intercepted Message

. . . and detectes eavesdropping



Probability of detecting Eve

All in all Alice and Bob detect eavesdropping with the probability of $\frac{1}{2} \cdot (1 - \frac{1}{2}) = \frac{1}{4}$.

Theorem

Using n bits to detect eavesdropping Alice and Bob will detect Eve with probability $1 - \left(\frac{3}{4}\right)^n$.

Example

In our example: $n = 10$
Probability of detecting Eve: $\approx 94,37\%$

Oulook

- Charles Bennett and Gilles Brassard constructed the first working prototyp at the IBM T.J. Watson Research Center in 1989. It worked over a distance of 30 cm.
- In 1995 swiss scientists established a quantum-connection between Genf and Lausanne.
  It was 67 km long and worked with 1kBit/s.
- In April 2004 the first money-transfer secured by quantum-encryption took place in Vienna.

Simon Singh:

At the current state it is possible to build a connection between the White House and the Pentagon. Perhaps there already is one.

Thank you for your Attention!